IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE

PLAINTIFF'S LOCAL RULE 56.1 STATEMENT OF UNDISPUTED FACTS IN OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

Pursuant to Rule 56 of the Federal Rules of Civil Procedure and Local Rule 56.1(b), Plaintiff Securities and Exchange Commission ("SEC") hereby submits its Local Rule 56.1 Statement of Undisputed Facts in Opposition to Defendants' Motion for Summary Judgment. The SEC's allegations that are at issue in that motion focus on false and misleading statements in a Security Statement that was posted to SolarWinds' public website, including during the Relevant Period of October 2018 to January 2021.

I. BACKGROUND ON SOLARWINDS SECURITY STATEMENT

1. SolarWinds is a provider of information technology ("IT") infrastructure management software, which enables organizations to monitor and manage the performance of their IT environments. [SEC Ex. 57 [SolarWinds Oct. 18, 2018 Form S-1], at 1].[1]

[1] The SEC's Memorandum of Law in Opposition to Defendants' Motion for Summary Judgment is referred to as "SEC Opp." The SEC's Rule 56.1 Statement of Undisputed Facts is referred to as "SEC 56.1." The SEC's Response and Counter-Statement to Defendants' Statement of Undisputed Material Facts is referred to as the "Response to Def. 56.1." Defendants'

2. Starting in November 2017 and continuing through December 14, 2020, SolarWinds maintained a written Security Statement that purported to provide readers with information about SolarWinds' cybersecurity infrastructure and practices. [JS ¶25].[2]

3. Among other things, the Security Statement described SolarWinds' purported cybersecurity procedures in areas including: (1) Access Controls; (2) Authentication and Authorization, which included password policy and password best practices; (3) Secure Development Lifecycle ("SDL"); and (4) Organizational Security, including use of the National Institute of Standards and Technology ("NIST") Cybersecurity Framework. [Ex. A to JS at 1, 3].

4. The Security Statement was available on SolarWinds' public facing website throughout the Relevant Period, including in October 2018 when SolarWinds conducted an initial public offering that raised approximately $460,000,000 and May 2019 when SolarWinds conducted a follow-on offering that raised approximately $326,715,000. [SEC Ex. 57 [SolarWinds Oct. 18, 2018 Form S-1], at 1; SEC Ex. 75 [SolarWinds May 20, 2019 Form S-1], at 1]. SolarWinds also had an employee stock purchase plan in effect throughout the Relevant Period. [SEC Ex. 79 [SolarWinds Form 10-K for 2020], at F-35].

5. The Security Statement remained on SolarWinds' website through December 14, 2020, when SolarWinds announced that it had suffered a significant cybersecurity attack, later dubbed SUNBURST. [JS ¶26; SEC Ex. 82 [SolarWinds Form 8-K filed December 14, 2020]].

Memorandum of Law In Support of Motion for Summary Judgment, ECF 184, is referred to as "Def. Br." Defendants' Rule 56.1 Statement of Undisputed Facts is referred to as "Def. 56.1." The Parties' Joint Statement of Undisputed Facts, ECF 166, is referred to as "JS." The Declaration of Kristen Warden in Opposition to Defendants' Motion for Summary Judgment is referred to as "Warden Decl."

[2] The SEC has, to a de-minimis extent, repeated certain facts from the Joint Statement of Undisputed Facts to provide context for other facts.

6. Throughout the Relevant Period, it was SolarWinds' practice to direct customers to the public facing Security Statement to answer questions regarding security practices. [SEC Ex. 19 [Bliss Dep.] 287:14-20].

II. BACKGROUND ON DEFENDANT TIMOTHY G. BROWN

7. Defendant Timothy G. Brown ("Brown") was hired by SolarWinds as Vice President of Security and Architecture in July 2017. [SEC Ex. 2 [Brown Dep.] 21:24-25, 29:21-22; SEC Ex. 19 [Bliss Dep.] 45:23-46:2; JS ¶15].

8. In that position, Brown supervised the SolarWinds Information Security ("InfoSec") team, which was comprised of approximately "five to eight" employees. [SEC Ex. 19 [Bliss Dep.] 27:1-25, 28:1-25, 29:6-18].

9. Part of the reason that Brown was hired in July 2017 was SolarWinds' recognition that, "given how the world was changing…we were going to need to invest in improving the overall cybersecurity posture of the company." [SEC Ex. 19 [Bliss Dep.] 50:21-51:4].

10. Throughout the Relevant Period, Brown was authorized by SolarWinds to make public statements "about cybersecurity generally." [SEC Ex. 19 [Bliss Dep.] 64:3-18, 65:1-11].

III. BROWN'S ROLE IN CONNECTION WITH THE SECURITY STATEMENT

11. Brown was a "proponent and sponsor" of the Security Statement. [SEC Ex. 2 [Brown Dep.] 57:19-22].

12. The Security Statement was drafted by Eric Quitugua, SolarWinds' Senior InfoSec Manager who reported directly to Brown. Brown reviewed the draft Security Statement from Mr. Quitugua to make sure that the statements were correct and provided feedback to Mr. Quitugua on what could be corrected. [SEC Ex. 2 [Brown Dep.] 57:23-58:14, 62:18-63:18, 63:23-64:6].

13. Brown had the ability to make changes to the draft Security Statement before it was finalized. [SEC Ex. 19 [Bliss Dep.] 74:12-18, 74:22-75:5; SEC Ex. 2 [Brown Dep.] 62:18-63:18].

IV. SOLARWINDS' INTERNAL DESCRIPTIONS OF ACCESS CONTROL DEFICIENCIES WERE INCONSISTENT WITH THE SECURITY STATEMENT.

14. The Security Statement described SolarWinds' purported Access Control practices as follows:

> **Access Controls**
>
> **Role Based Access**
>
> Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis. Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.
>
> **Authentication and Authorization**
>
> …SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes.

[Ex. A to JS at 3].

A. Internal SolarWinds Communications Prior to the IPO Demonstrated Practices That Contradicted the Representations in the Security Statement and Gave Defendants Notice of SolarWinds' Cybersecurity Problems.

15. In August 2017, shortly after Brown joined SolarWinds, Mr. Quitugua prepared a cybersecurity assessment to "establish some kind of baseline to work off of so that

[SolarWinds] could generate some kind of roadmap on improving the security program, you know, moving forward." [SEC Ex. 25 [Quitugua Dep.] 190:15-21]. Mr. Quitugua explained that when he referred to baseline, he meant the "current state" of cybersecurity "at a point in time." [SEC Ex. 25 [Quitugua Dep.] 190:22-25].

16. That same month, a PowerPoint presentation titled "Monthly IT Leadership Meeting" included a "Security State of the Union," slide prominently featuring a picture of Brown [SEC Ex. 12 [SW-SEC00259782-9803], at -9786].

17. That presentation described SolarWinds' need to "Lock down administrative access" and "Implement security training for all employees." [*Id.* at -9787].[3]

18. As per the metadata for the document, SolarWinds' Chief Information Officer ("CIO"), Rani Johnson, was the custodian of the document. [*Id.* at PDF page *5; *see also* JS ¶¶159-160 (additional quotes from same document)].

19. In September 2017, Brown emailed a presentation stating, "[c]urrent state of security and proposed move to a proactive security model." [SEC Ex. 83 [SW-SEC00337355-7362], at -7355, -7356-7362; *see also* JS ¶161]. One of the slides in this presentation stated, "Risk of Non-Investment," which stated: "[c]urrent state of security leaves us in a very vulnerable state for our critical assets. A compromise in these assets would damage our reputation and financially [sic]." [SEC Ex. 83 [SW-SEC00337355-7362], at -7360; *see also* JS ¶161].

i. March 2018 Major Projects Portfolio

20. On March 16, 2018, Brad Cline, who served as the Director of Information Technology and Senior Director of Information Technology during the Relevant Period, emailed Ms.

[3] References to "administrator rights," "administrative rights," "admin rights," and "administrative access" are interchangeable.

Johnson an updated draft PowerPoint entitled "Major Project Portfolio" (hereafter "March 2018 Major Project Portfolio." [SEC Ex. 14 [SW-SEC00042892-2964]; SEC Ex. 66 [Cline Dep.] 12:13-17, 18:17-23].

21. Mr. Quitugua contributed to particular slides within the March 2018 Major Project Portfolio, including a slide that discussed conducting a security assessment and remediation in preparation for GDPR. [SEC Ex. 14 [SW-SEC00042892-2964], at -2906; SEC Ex. 25 [Quitugua Dep.] 201:5-203:10, 208:20-24].

22. He also contributed to a slide titled, "Enterprise Access Management (Standards & Audit)." [SEC Ex. 14 [SW-SEC00042892-2964], at -2907; SEC Ex. 25 [Quitugua Dep.] 216:2-13].

23. The general purpose of these types of presentations was to track SolarWinds' ongoing projects, SEC Ex. 66 [Cline Dep.] 146:15-20, and the intended audience for the March 2018 Major Project Portfolio was Ms. Johnson and her leadership team. [SEC Ex. 25 [Quitugua Dep.] 211:14-25, 225:15-226:1].

24. Among other things, the "Enterprise Access Management (Standards & Audit)" Slide stated, "Concept of least privilege not followed as a best practice." [SEC Ex. 14 [SW-SEC-00042892-2964], at -2907].

25. Although Mr. Quitugua could not "distinctly recall" particular instances of the concept of least privilege not being followed at SolarWinds, he admitted that "that could have very well been raised as a concern," and that as part of an internal assessment, "it may have been found that a particular system wasn't following the concept." [SEC Ex. 25 [Quitugua Dep.] 218:20-220:10].

26. The "Enterprise Access Management (Standards & Audit)" slide of the March 2018 Major Project Portfolio also listed as an "Action Required" that SolarWinds needed to "Work with teams to decommission use of shared accounts." [SEC Ex. 14 [SW-SEC00042892-2964], at -2907; JS ¶184]. Generally, this describes an account that it shared, either by users or " sometimes an account different from a human account can be used by a computer to perform its function. And that same service account—or account could be used in a different computer, again, doing the same function to do its job as well." [SEC Ex. 25 [Quitugua Dep.] 221:8-23]. Mr. Quitugua did not recall what "shared accounts" in the particular context of this slide meant. [SEC Ex. 25 [Quitugua Dep.] 220:25-221:7].

27. Decommissioning the use of shared accounts meant "[t]o basically disable the account or separate the use of that account by multiple systems or multiple people." [SEC Ex. 25 [Quitugua Dep.] 223:9-13; SEC Ex. 14 [SW-SEC00042892-2964], at -2907].

28. The "Enterprise Access Management (Standards & Audit)" slide also stated under the subheading "Action Required" that SolarWinds needed to "ID existing permission levels within the enterprise." [SEC Ex. 14 [SW-SEC-00042892-2964], at -2907; JS ¶184].

29. The Notes to the "Enterprise Access Management (Standards & Audit)" slide of the March 2018 Major Project Portfolio stated in part: "10/16/17 Update - Identity management continues to be a concern. Appropriate checks are in place to grant access but audit of access is not consistently implemented. Multi-Factor authentication should also be utilized in more environments. A risk assessment will be completed by 12/31." [SEC Ex. 14 [SW-SEC-00042892-2964], at -2907].

30. A prior version of the March 2018 Major Project Portfolio that Brown emailed to Mr. Quitugua on March 15, 2018 contained many of the same notes as described above, including

that the "Concept of least privilege is not followed as a best practice." [SEC Ex. 32 [SW-SEC00012265-2275], at -2268].

ii. April 2018 Audit

31. An April 13, 2018 email from Ms. Johnson to Brown, Mr. Quitugua, David Mills, Kellie Pierce, and Joel Kemmerer including April 2018 audit results stated that "[s]hared SQL legacy account login credentials [were] used" for three business units. [SEC Ex. 33 [SW-SEC00043080-3084], at 3080-3083].

32. On April 13, 2018, Mr. Mills forwarded Ms. Johnson's email to Mr. Cline, Mr. Quitugua, and Smitha Reddy. [SEC Ex. 33 [SW-SEC00043080-3084], at -3080]. Mr. Cline responded: "my understanding is these are old [SQL] accounts that are shared among multiple [databases]/websites and pose a security risk." [SEC Ex. 33 [SW-SEC00043080-3084], at -3080; JS ¶185].

iii. September 2018 Presentation

33. A September 2018 presentation entitled "Bi-Weekly DOIT Staff Meeting," for which Ms. Johnson was the custodian included a slide titled "SOX Controls: Findings Summary" whose subtitle was "#notwinning." The slide documented that for "User Access Management," of the 7 controls reviewed only 3 were in place with 4 "Partially in Place." A frowny-face emoji appears next to the "Not in Place" and "Partially in Place" assessments. [SEC Ex. 16 [SW-SEC00310427-0447] at -0440 (quotes) and PDF page *5 (metadata)].

B. A Significant Security Gap Identified by SolarWinds' Network Engineer Robert Krajcir in June 2018 Was Communicated to Brown and Persisted into the Relevant Period.

34. On June 4, 2018, Network Engineer Robert Krajcir emailed multiple people, including Mr. Cline and Mr. Quitugua, identifying: "a "security gap" relating to SolarWinds' remote access through a virtual private network ("VPN"), which allowed access from devices not

managed by SolarWinds. Mr. Krajcir warned that this setup was "not very secure." [SEC Ex. 15 [SW-SEC00031653-1668], at -1657; *see also* JS ¶¶168-170].

35. Mr. Krajcir proposed that SolarWinds "[u]se certificates for machine authentication." [SEC Ex. 15 [SW-SEC00031653-1668], at -1657; *see also* JS ¶166].

36. Mr. Krajcir explained that under his proposal, "users will only be able to connect to our VPN from verified/trusted devices, that are under IT control, joined the domain, are properly updated and have the required software properly installed and in use." [SEC Ex. 15 [SW-SEC00031653-1668], at -1657; *see also* JS ¶166].

37. On June 5, 2018, Mr. Krajcir emailed Mr. Cline, Mr. Quitugua, and others and stated, "[I]n my point of view, vendors, or non-domain computers in general should not have unrestricted access to our network, and thus should fall under one of the restricted categories that does not need any certificates." [SEC Ex. 15 [SW-SEC00031653-1668], at -1656].

38. Mr. Krajcir also stated, "Users accessing our VPN from company-owned device – should use machine certificate to authenticate their PC." [SEC Ex. 15 [SW-SEC00031653-1668], at -1656].

39. On August 24, 2018, Mr. Krajcir sent a follow-up email to multiple people, including Mr. Cline and Mr. Quitugua, asking to "drag your attention back to this topic." In his email, Mr. Krajcir wrote: "Implementing certificates is essential to enforce proper security policies not only on VPN, but also on corporate wireless, to properly address BYOD problem." [SEC Ex. 15 [SW-SEC00031653-1668], at -1654].

40. In that email, Mr. Krajcir identified four "risk[s]" that SolarWinds was facing: (1) "Anyone with AD credentials can access our corporate wifi or corporate VPN from ANY device, no matter if [C]ompany owned or not;" (2) "While on corporate wifi, or VPN, such

device can basically do whatever without us detecting it until it's too late" (3) "It can easily download any content without being detected by NetScope [SolarWinds' data loss prevention software], which is normally installed on all domain PCs;" and (4) "[I]t can compromise entire network by spreading malware (spyware, viruses, trojans, ransomware), because we cannot ensure that such device will be fully compliant in terms of [operating system] updates, antivirus [protection], software installed, etc." [SEC Ex. 15 [SW-SEC00031653-1668], at -1654; *see also* JS ¶168].

41. On August 30, 2018, Mr. Krajcir sent a follow-up email to multiple people, including Mr. Cline and Mr. Quitugua, thanking them for attending a meeting and attaching a copy of a PowerPoint presentation entitled "BYOD solution, Machine certificate authentication" (the "BYOD Presentation") that Mr. Krajcir presented at the meeting. [SEC Ex. 15 [SW-SEC00031653-1668], at -1653, -1659, -1668].

42. Mr. Krajcir was listed as the author of the PowerPoint presentation. [SEC Ex. 15 [SW-SEC00031653-1668], at -1659].[4]

43. On the "Current Status" slide of the BYOD Presentation, it stated, among other things: (1) "No means to enforce or monitor what devices connect to our network;" (2) "No options how to guarantee user identity;" and (3) "Employees do not respect security guidelines, [including] [i]nstalling 3rd party software, even games…using torrents [and] connect own devices or phones to SolarWinds SSID instead of guest." [SEC Ex. 15 [SW-SEC00031653-1668], at -1661; *see also* JS ¶168]

[4] The Parties' Joint Statement of Undisputed Facts, ECF No. 166, incorrectly identified the August 2018 "BYOD Solution, Machine Certificate Authentication" presentation as an attachment to Mr. Krajcir's June 4, 2018 email. [JS ¶166]. The presentation was actually attached to and referenced in Mr. Krajcir's August 30, 2018 email. [SEC Ex. 15 [SW-SEC00031653-1668] at -1653, -1658-1659, -1668].

44. On the "Risks for Company" slide, the BYOD Presentation stated, among other things: "[T]here will be major reputation and financial loss to the company." [SEC Ex. 15 [SW-SEC00031653-1668], at -1662].

45. On the "Implementing Certificates" slide, it stated, along other things: "Manage user admin rights[:] At this time basically unlimited." [SEC Ex. 15 [SW-SEC00031653-1668], at -1665].

46. This slide also stated: "Implement certificate authentication[:] Machine only authentication." [SEC Ex. 15 [SW-SEC00031653-1668], at -1665].

47. Mr. Quitugua forwarded a copy of the presentation to Brown on August 31, 2018. [SEC Ex. 67 [SW-SEC00594395-4410], at -4395; *see also* JS ¶170].

48. Despite Mr. Krajcir's attempts, as of January 2020, SolarWinds had not implemented Mr. Krajcir's suggestion for implementing machine-based authentication for the global protect VPN. [SEC Ex. 25 [Quitugua Dep.] 257:15-23].

49. On January 16, 2020, Mr. Quitugua emailed Brown, copying Mr. Krajcir, explaining that the recommendations from Mr. Krajcir's presentation "did not get any traction" and asking if "we can circle this back and see if we can re-assess and possibly implement some type of enforcement." [SEC Ex. 53 [SW-SEC00666779-6784], at -6779]. Mr. Krajcir replied, confirming that, regarding global protect VPN, "we are still standing on the same spot. Anyone can connect from anywhere as long as they know AD credentials." [*Id.*].

50. Mr. Quitugua did not recall whether SolarWinds took any further action as a result of Mr. Krajcir's August 2018 email or in response to his follow-up to Brown. [SEC Ex. 25 [Quitugua Dep.] 253:22-257:14, 262:9-12, 339:20-340:16].

51. On January 12, 2021, following discovery of the SUNBURST attack, SolarWinds IT Manager Eric Houston emailed Mr. Cline regarding "Corporate Network Security Recommendations" in response to Mr. Cline's request that Mr. Houston "review the infrastructure design and security best practices and make recommendations." [SEC Ex. 80 [SW-SEC00522109-2122], at -2109-2110].

52. Mr. Houston's recommendations, which were included in the email and attached presentation, included many of the same recommendations that Mr. Krajcir raised years earlier. [*Compare* SEC Ex. 80 [SW-SEC00522109-2122], at -2109, -2116, -2118; *with* SEC Ex. 15 [SW-SEC00031653-1668], at -1657, -1664-1665].

53. The recommendations included: (1) "Prove SolarWinds asset [v]ia machine certificate, installed;" (2) "SolarWinds official corporate devices can be connected to wired L[ocal] A[rea] N[etwork]... All other devices should be forbidden;" (3) "[O]nly corporate approved devices should be allowed VPN access;" (4) "VPN should use two factor authentication;" (5) "Non-SolarWinds access for VPN [s]hould have only limited access to needed resources - in specific secured zone." [SEC Ex. 80 [SW-SEC00522109-2122], at -2109, -2116, -2118].

54. Mr. Houston's email shows that SolarWinds still had not, in January 2021, remedied the problems that Mr. Krajcir had identified in 2018. [*Compare* SEC Ex. 80 [SW-SEC00522109-2122]; *with* SEC Ex. 15 [SW-SEC00031653-1668]].

C. Brown Was Aware of Significant Access Control Deficiencies that Contradicted the Security Statement at the Time of SolarWinds IPO.

55. In September 2017, Brown emailed a presentation stating, "[c]urrent state of security and proposed move to a proactive security model." [SEC Ex. 83 [SW-SEC00337355-7362], at -7355, -7356-7362; *see also* JS ¶161]. One of the slides in this presentation stated, "Risk of Non-Investment," which stated: "[c]urrent state of security leaves us in a very vulnerable state

for our critical assets. A compromise in these assets would damage our reputation and financially [sic]." [SEC Ex. 83 [SW-SEC00337355-7362], at -7360; *see also* JS ¶161].

56. In October 2018, Brown prepared a draft presentation titled "Information Security - Risk Review." [SEC Ex. 18 [SW-SEC00313350-3362], at -3351; SEC Ex. 2 [Brown Dep.] 163:8-164:23].

57. This was an update of the August 2017 and September 2017 presentations referred to in JS ¶¶159-161. [SEC Ex. 18 [SW-SEC00313350-3362]; SEC Ex. 12 [SW-SEC00259782-9803], at -9782; SEC Ex. 83 [SW-SEC00337355-7362], at -7356-7352].

58. In his deposition, Brown acknowledged that it was a routine practice to provide Ms. Johnson with updates on the state of SolarWinds security operations, and the October 2018 presentation titled "Information Security - Risk Review" was one example of the information he provided to Ms. Johnson. [SEC Ex. 2 [Brown Dep.] 164:14-23].

59. Under the slide "A Proactive Security Model – Updated October 2018 with status," Brown identified as a "Risk of Non-Investment" that the "[c]urrent state of security leaves us in a very vulnerable state for our critical assets," color-coded in yellow. [SEC Ex. 18 [SW-SEC00313350-3362], at -3361].

60. In testifying about a prior version of this slide, Brown acknowledged it contained the same "very vulnerable state for our critical assets" language as the October 2018 presentation, [SEC Ex. 3 [SW-SEC00262716-2743], at -2743; SEC Ex. 2 [Brown Dep.] 289:12-25]. Brown claimed in testimony that he was engaging in "puffery" when he said the "current state of security leaves us in a very vulnerable state for our critical assets," but then when testifying about the October 2018 version of that statement he said it was simply carried over from the earlier presentation and that he did "not recall his state of mind" when he made the original

statement in 2017 (that was repeated in the 2018 presentation). [SEC Ex. 2 [Brown Dep] 150:11-20, 156:22-157:15, 289:3-8, 289:12-25; SEC Ex. 18 [SW-SEC00313350-3362], at -3359; SEC Ex. 3 [SW-SEC00262716-2743], at -2743].

61. Brown also did not recall the details of why he put that statement in yellow in the October 2018 presentation [SEC Ex. 2 [Brown Dep] 167:3-22].

62. Brown also could not recall which tasks had been performed as of October 2018 with respect to the reference to the "current state of security leaves us in a very vulnerable state for our critical assets." [SEC Ex. 2 [Brown Dep] 167:23-168:11].

63. When asked about the slide's reference to, "very vulnerable risk," Mr. Bliss claimed it was "hyperbole" and also claimed that while Brown was "identifying a risk," it was "not a factual finding." [SEC Ex. 19 [Bliss Dep.] 219:21-221:5; *see also* Brown Decl. ¶4 (stating there was "room for improvement" in SolarWinds cybersecurity program and that his comments on the slide were "merely hyperbole" beyond that)].

64. On October 3, 2018, Mr. Quitugua sent a security incident status summary to SolarWinds' Chief Technology Office Joe Kim, Ms. Johnson, and Brown. That document noted that the Orion Platform (a flagship product and "very important platform for the SolarWinds company") currently "Lacks Proper Access Controls" and that "[p]laintext credentials for access to configured nodes [were] exposed in HTML source code" of Orion NCM. [SEC Ex. 68 [SW-SEC-SDNY_00006396]; SEC Ex. 43 [Kim Dep.] 231:16-22, 235:25-237:2].

65. Orion was the system into which attackers injected malicious code as part of the SUNBURST attack. [SEC Ex. 79 [SolarWinds (1 March 2020), Form 10-K for 2020], at 2].

D. Additional Access Control Problems Persisted Following SolarWinds' IPO and Were Communicated to Brown and Other Executives.

66. A December 2018 Security Operations Summary, on a slide titled "Security Projects Key Areas to Address Gaps in Information Security" included the following "Gap Analysis" for the yellow-highlighted "Focus Area" titled "Privilege Access Management (PAM) and Multifactor Authentication": "Address the use of local administrator access to non-privileged users. Manage, audit, and apply security controls around privileged access." [SEC Ex. 20 [SW-SEC00638663-8677], at -8674].

67. Brown testified that "[a]dministrative rights to their local desktop, laptop were granted…for essentially everyone at this stage." [SEC Ex. 2 [Brown Dep.] 216:1-11].

68. Local administrator (or administrative) rights gave employees the ability to install "anything" on their own devices. [SEC Ex. 2 [Brown Dep.] 217:10-14 ("Q. Okay. If someone were to install mal-ware on their own device, would they be able to do that on their own device if they had local administrator rights? A. So they could, yes. They could install anything.")].

69. Brown testified that because local administrative rights were granted to all employees, SolarWinds had to rely on "a number of safeguards in place against mal-ware." [SEC Ex. 2 [Brown Dep.] 217:10-18, 218:4-8].

70. The May 17, 2019 Security & Compliance Program Quarterly had a slide titled "Security & Compliance Initiatives." [SEC Ex. 21 [SW-SEC00001635-1652], at -1641].

71. On that slide, under the initiative "Security Incident Improvement Plan (SIIP)," it stated, "[e]ffort working with the entire organization to improve the overall security posture, reduce incidents and monitor progress." [SEC Ex. 21 [SW-SEC00001635-1652], at -1641].

72. On another slide in that same presentation titled "Security: Security Incident Improvement Plan (SIIP)," it described a "[p]roject to operationalize and improve overall security for SolarWinds." [SEC Ex. 21 [SW-SEC00001635-1652], at -1650].

73. On that slide, under "Description," the slides states: "This effort includes training (security and SDL), department plans for addressing security, KPIs and an annual audit to measure the effectiveness of security practices within SolarWinds." [SEC Ex. 21 [SW-SEC00001635-1652], at -1650].

74. That same May 17, 2019 Security & Compliance Program Quarterly presentation also had a slide titled "Financial: Enterprise Access Management (SOX Compliance)." [SEC Ex. 21 [SW-SEC00001635-1652], at -1644].

75. Under the category of "Issues, Risks, & Dependencies," that slide stated: "Concept of least privilege not followed as a best practice." [SEC Ex. 21 [SW-SEC00001635-1652], at - 1644].

76. This slide also identified under "Issues, Risks, and Dependencies" the "Use of shared accounts throughout internal and external applications" with an action item to "Work with teams to decommission use of shared accounts." [SEC Ex. 21 [SW-SEC00001635-1652], at -1644].

i. August 2019 Security & Compliance Program Quarterly Overview

77. A SolarWinds August 16, 2019 Security & Compliance Program Quarterly Overview, which were comprised of Ms. Johnson's initiatives, contained a slide titled: "SolarWinds Scorecard: NIST Maturity Level." [SEC Ex. 5 [SW-SEC00001497-1550], at -1505; SEC Ex. 2 [Brown Dep.] 183:13-184:20; *see also* JS ¶177 (containing further detail)].

78. This presentation stated, "need to improve internal processes/procedures." [SEC Ex. 5 [SW-SEC00001497-1550], at -1507].

79. The presentation also had a slide titled "Financial: Enterprise Access Management (SOX Compliance)." [SEC Ex. 5 [SW-SEC00001497-1550], at -1523]. Under the category of "Issues, Risks, & Dependencies," that slide stated: "Concept of least privilege not followed as a best practice," and "Use of shared accounts throughout internal and external applications." [SEC Ex. 5 [SW-SEC00001497-1550], at -1523]. The slide also stated "[n]eed to assess existing controls to ensure alignment with SOX requirements." [SEC Ex. 5 [SW-SEC00001497-1550], at -1523].

80. This presentation was likely intended for a SolarWinds executive audience. [SEC Ex. 19 [Bliss. Dep.] 225:18-226:4].

81. The August 2019 Security & Compliance Program Quarterly Overview presentation was the first time the NIST maturity level scorecard format was reported to SolarWinds senior management. [SEC Ex. 5 [SW-SEC00001497-1550]; SEC Ex. 19 [Bliss Dep.] 227:5-19].

82. The purpose of the SolarWinds' Security Scorecards was "[t]o establish a security baseline," and "review…specific security controls and how teams, groups, the organization within the company adhere to those guidelines or controls or not." [SEC Ex. 25 [Quitugua Dep.] 38:18-39:5].

83. The Security Scorecards were prepared in connection with the NIST cybersecurity framework guidelines. [SEC Ex. 25 [Quitugua Dep.] 39:6-10].

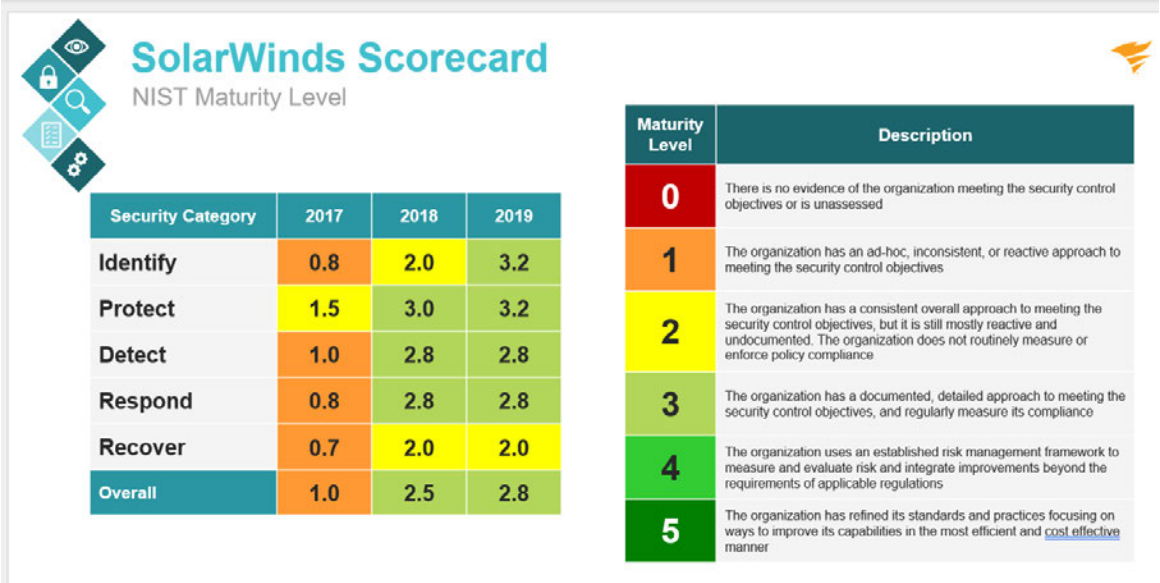
84. Mr. Kim reviewed a copy of the August 16, 2019 Security & Compliance Program Quarterly Overview presentation emailed to him by Ms. Johnson. [SEC Ex. 70 [SW-SEC00264310-4364]; SEC Ex. 43 [Kim Dep.] 238:3-240:20].

85. The presentation included an assessment of NIST maturity level for the years 2017, 2018, and 2019 on a scale of 0 through 5, with a 1.0 indicating that the organization had an ad

hoc inconsistent or reactive approach to meeting the security control objectives. [SEC Ex. 70 [SW-SEC00264310-4364], at -4319; SEC Ex. 43 [Kim Dep.] 243:20-244:5]."

86. The August 16, 2019 Security & Compliance Program Quarterly Overview's assessment of NIST maturity level, within the "Protect" category, for the subcategory "Authentication, Authorization and Identity Management" (with an objective of "User identity, authentication and authorization are in place and actively monitored across the company" was "1." [SEC Ex. 70 [SW-SEC00264310-4364], at -4321].

87. The August 16, 2019 Security & Compliance Program Quarterly Overview's assessment of NIST maturity level for the years 2017, 2018, and 2019, SEC Ex. 70 [SW-SEC00264310-4364], at -4319, were:



SolarWinds Scorecard

NIST Maturity Level

Security Category	2017	2018	2019
Identify	0.8	2.0	3.2
Protect	1.5	3.0	3.2
Detect	1.0	2.8	2.8
Respond	0.8	2.8	2.8
Recover	0.7	2.0	2.0
Overall	1.0	2.5	2.8

Maturity Level	Description
0	There is no evidence of the organization meeting the security control objectives or is unassessed
1	The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives
2	The organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance
3	The organization has a documented, detailed approach to meeting the security control objectives, and regularly measure its compliance
4	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations
5	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost effective manner

88. The August 16, 2019 Security & Compliance Program Quarterly Overview included a statement that "Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures." [SEC Ex. 70 [SW-SEC00264310-4364], at -4321; *see also* JS ¶177].

89. Ms. Johnson has given two contradictory explanations for this language. In her declaration she said "[the bullet about '[a]cess and privilege to critical systems/data' being 'inappropriate' was a shorthand reference to access being managed in a way that was decentralized at a technical level—which created a risk of error, as discussed above. Again, we wanted to minimize this risk through migrating to centralized, automated tooling like Azure AD." [Johnson Decl. ¶14]. But in her deposition, Ms. Johnson testified that it was a "summarized highlight pointing to the opportunity to leverage technology called Thycotic Secret Server to mid – to manage privileged access credentials in a secret server." [SEC Ex. 10 [SW-SEC00305126-5155], at -5148; SEC Ex. 52 [Johnson Dep.] 175:3-18].

90. Brown has also given changing and contradictory explanations for this statement. At his deposition, Brown testified that he did not "recall that specific statement or what it was in reference to." [SEC Ex. 2 [Brown Dep.] 202:15-25]. But then, in Brown's declaration (prepared after his deposition), he said that he "reviewed Ms. Johnson's Declaration on this topic and agree with her statements." [Brown Decl. ¶¶8-9]. Ms. Johnson's declaration described the reference to "Access and privilege to critical systems/data is inappropriate" as relating to "the Company's ongoing efforts at this time to centralize and automate its access control tooling, including in particular the migration to Azure AD." [Johnson Decl. ¶¶11-13; *see* Def. Br. at 27-29]. Ms. Johnson's declaration also stated that this reference was "a shorthand reference to access being managed in a way that was decentralized at a technical level−which created the risk of error." [Johnson Decl. ¶14]. Brown's declaration parroted most of Ms. Johnson's declaration on this topic, stating: "[O]ur focus during the Relevant Period was on migrating to a new Identity and Access Management ("IAM") solution—Microsoft Azure Active Directory ("Azure AD")…We were also working to roll out a Privileged Access

Management ("PAM") solution known as "Thycotic," which provides specialized tooling to manage access to privileged accounts." [Brown Decl. ¶9].

91. In addition, when asked during his deposition whether he knew what the phrase in the August 16, 2019 Security & Compliance Program Quarterly Overview—"critical systems/data"—referred to, Brown testified "[n]ot at all." [SEC Ex. 2 [Brown Dep.] 204:6-8; SEC Ex. 70 [SW-SEC00264310-4364], at -4321].

92. Brown also testified that he did not know what the phrase "[a]ccess and privilege" meant. [SEC Ex. 2 [Brown Dep.] 204:9-11; SEC Ex. 70 [SW-SEC00264310-4364], at -4321].

ii. FedRAMP Assessment Spreadsheets

93. Three spreadsheets titled "FedRAMP_Security_Controls_Baseline," which were compiled by SolarWinds employee Ms. Pierce in June, August, and September of 2019, identified numerous instances where SolarWinds' access control policies did not meet the standards of NIST 800-53.[5] [SEC Ex. 22 [SW-SEC00151673-1675]; SEC Ex. 23 [SW-SEC00045356-5358]; SEC Ex. 24 [SW-SEC00218068-8069]].

94. Among other findings, the June FedRAMP Assessment includes assessments stating the following for the control name "least privilege/authorize access to security functions:" "The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]," [SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *5, line 17], for which Ms. Pierce's comment was "[w]e have no explicit authorization policy, nor is this documented that I am

[5] Each "FedRAMP Security Controls Baseline" spreadsheet is designated by the month the spreadsheet was prepared and the description "FedRAMP Assessment." The "FedRAMP Security Controls Baseline" spreadsheets are collectively referred to as the "FedRAMP Assessments."

aware of for the company or individual products." [SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *5, line 17].

95. The June FedRAMP Assessment prepared by Ms. Pierce also contained findings about the status of other pertinent controls. For the topic, "organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles[,]" Ms. Pierce's comment was: "[w]e have no explicit restriction policy, nor is this documented that I am aware of for the company or individual products." [SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *5, line 19].

96. For the topic, "the organization [e]stablishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices," the June FedRAMP Assessment found: "[C]ompany does not have a policy on non-network devices connecting to the network." [SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *6, line 37].

97. For the topic, "[t]he organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information," the June FedRAMP Assessment found: "The company does not have an access control for mobile devices." [SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *6, line 38].

98. For the topic, "[t]he organization... [f]acilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information," the June FedRAMP Assessment found: "[A]uthorized vs. unauthorized users has not been defined and policies are not fully comprehensive to meet this control." [SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *7, line 42].

99. For the topic "[t]he organization... [l]imits privileges to change information system components and system-related information within a production or operational environment," and "[r]eviews and reevaluates privileges," the June FedRAMP Assessment found: "[n]o known privilege limitations." [SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *8, line 94].

100. Each of the findings (as set forth in paragraphs 94 to 99 above) indicate in column J of the spreadsheet that they relate to a "Process." [SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *5, line 17, column J in native version; SEC Ex. 22 [SW-SEC00151673-1675], PDF page *5, line 19, column J in native version; SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *6, line 37, column J in native version; SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *6, line 38, column J in native version; SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *7, line 42, column J in native version; SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *8, line 94, column J in native version].

101. That these findings (as set forth in paragraphs 94 to 99 above) relate to a process means that they relate to an internal SolarWinds security procedure (or lack thereof) not to a product that SolarWinds produced for customer usage. [SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *5, line 17, column J in native version; SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *5, line 19, column J in native version; SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *6, line 37, column J in native version; SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *6, line 38, column J in native version; SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *7, line 42, column J in native version; SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *8, line 94, column J in native version].

iii. March 2020 Quarterly Risk Review

102. A SolarWinds March 3, 2020 Quarterly Risk Review that was drafted with input from Brown and shared with SolarWinds' CIO and CTO, who in turn updated SolarWinds' CEO, contained a SolarWinds "scorecard" for NIST Maturity Level. [SEC Ex. 2 [Brown Dep.] 232:22-233:25].

103. Bliss testified that SolarWinds Quarterly Risk Reviews were discussed quarterly by "the CFO, myself, Joe Kim, Rani [Johnson]… and then Tim [Brown] and members of the various teams." [SEC Ex. 8 [SW-SEC00001608-1634], at -1611; SEC Ex. 19 [Bliss Dep.] 226:8-14, 247:17-21; *see also* JS ¶181].

104. The slide titled "SolarWinds Scorecard: NIST Maturity Level" in the March 2020 Quarterly Risk Review identified the following "key risks": "[s]ignificant deficiencies in user access management" and "[s]ecurity processes not consistently implemented." [SEC Ex. 8 [SW-SEC00001608-1634], at -1611; *see also* JS ¶181].

105. In his deposition, Brown claimed that the reference to "[s]ignificant deficiencies in user access management" was not "a finding" and was "simply a statement." [SEC Ex. 2 [Brown Dep.] 237:5-24].

iv. May 2020 Quarterly Risk Review

106. A SolarWinds May 22, 2020 Quarterly Risk Review also contained a SolarWinds "scorecard" for NIST Maturity Level. [SEC Ex. 7 [SW-SEC00001602-1607], at 1605; *see also* JS ¶182].

107. Mr. Quitugua recognized the NIST scorecard slide during his deposition, and he routinely provided input on this slide in presentations. [SEC Ex. 25 [Quitugua Dep.] 297:17-299:23].

108. The NIST Scorecard slide identified the following "key risks": "[s]ignificant deficiencies in user access management" and "[s]ecurity processes not consistently implemented." [SEC Ex. 7 [SW-SEC00001602-1607], at 1605; *see also* JS ¶182].

v. October 2020 Quarterly Risk Review

109. A SolarWinds October 27, 2020 Quarterly Risk Review also contained a SolarWinds "scorecard" for NIST Maturity Level. [SEC Ex. 9 [SW-SEC00001582-1601], at 1587; *see also* JS ¶182].

110. Brown recalled that his involvement in the October 27, 2020 Quarterly Risk Review was similar to his involvement in the Security & Compliance Program Overviews: he participated in meetings with Ms. Johnson and Ms. Pierce to discuss the content of these presentations. [SEC Ex. 2 [Brown Dep.] 222:20-223:2, 232:22-233:25, 246:7-246:21].

111. The NIST Scorecard slide identified the following "key risks": "[s]ignificant deficiencies in user access management" and "[s]ecurity processes not consistently implemented." [SEC Ex. 9 [SW-SEC00001582-1601], at 1587]; *see also* JS ¶183.

vi. Other Document

112. SolarWinds used a tool known as "Security Event Manager" or "SEM" to monitor SolarWinds' network. [JS ¶95].

113. However, a December 21, 2020 document, whose metadata indicates that it was prepared by Mr. Quitugua, shows that the notification that SEM sent was not necessarily an alert to the InfoSec team about whether an admin account change was correct or incorrect, only the fact of the change. [SEC Ex. 69 [SW-SEC-SDNY_00054914]; *id.* at PDF page *3 (metadata)].

114. This process did not allow the InfoSec team to automatically catch incorrect admin access changes. [SEC Ex. 69 [SW-SEC-SDNY_00054914]].

E. SolarWinds' SOX Audits For 2019 and 2020 Identified Deficiencies in SolarWinds' IT General Controls During the Relevant Period.

i. Background on Audits at SolarWinds

115. Beginning in at least Fiscal Year 2019, SolarWinds conducted internal audits of the company's compliance with Sarbanes-Oxley ("SOX") controls as they related to SolarWinds' access controls. [SEC Ex. 19 [Bliss Dep.] 257:22-258:18; SEC Ex. 52 [Johnson Dep.] 251:6-13; SEC Ex. 28 [SW-SEC00388330-8332 and attachment], at -8330; SEC Ex. 8 [SW-SEC00001608-1634], at -1618].

116. This was part of the SOX initiative at SolarWinds, and Ms. Johnson explained that some SOX objectives "align[ed] to security objectives." [SEC Ex. 19 [Bliss Dep.] 235:11-18; SEC Ex. 52 [Johnson Dep.] 252:7-13].

117. SolarWinds audited its access controls "to make sure that we were implementing them in the right manner." [SEC Ex. 19 [Bliss. Dep.] 257:22-258:18].

118. Internal SOX audits were supervised by Danielle Campbell, and Ms. Campbell's team was "guided by a set of auditors who participated in consulting [SolarWinds] in internal audit." [SEC Ex. 52 [Johnson Dep.] 251:14-25].

119. SolarWinds' internal SOX audits examined "IT General Controls," among other controls. [SEC Ex. 52 [Johnson Dep.] 254:21-255:4; SEC Ex. 28 [SW-SEC00388330-8332], at -8330, PDF page *4].

120. The "IT General Controls" relate to "change management and access management." [SEC Ex. 52 [Johnson Dep.] 254:21-255:8].

121. SolarWinds executives, including its General Counsel and Chief Financial Officer, received "briefings on SOX control deficiencies" which identified at a higher level a summary of audit findings related to access controls. [SEC Ex. 19 [Bliss Dep.] 259:1-9; SEC Ex. 52 [Johnson Dep.] 252:14-21].

ii. Internal FY2019 Audit

122. SolarWinds' fiscal year ends on December 31 of the calendar year. [*See, e.g.*, SEC Ex. 79 [SolarWinds Form 10-K for 2020], at 1].

123. In and around March 2020, SolarWinds finalized an audit of fiscal year 2019 that included findings regarding access controls and other cybersecurity matters. [SEC Ex. 28 [SW-SEC00388330-8332]; SEC Ex. 19 [Bliss Dep.] 257:22-260:8].

124. On March 2, 2020, Danielle Campbell emailed Chris Day, Ms. Johnson, and others with the subject "SOX: Control Deficiencies FY19" and she attached an excel spreadsheet with the file name "FY2019 Deficiencies and Recommendations – Final." [SEC Ex. 28 [SW-SEC00388330-8332] at -8332]; SEC Ex. 19 [Bliss Dep.] 257:22-260:8].

125. The email and attachment were "part of the auditing of access controls that [SolarWinds] would do to make sure that [SolarWinds was] implementing them in the right manner." [SEC Ex. 19 [Bliss Dep.] 257:22-258:18].

126. In her March 2, 2020 email, Ms. Campbell wrote: "There were 20 controls that were not remediated by yearend. I would like to have all of these remediated in Q1 or early Q2." [SEC Ex. 28 [SW-SEC00388330-8332], at -8330].

127. 10 of the unremediated controls were "IT general controls." [SEC Ex. 28 [SW-SEC00388330-8332], at -8330].

128. The attachment listed Brown as the "control owner" for two of the deficiencies, including that for two servers (of four tested) "password complexity was not enforced." [SEC Ex. 28 [SW-SEC00388330-8332], at PDF page *5; *see* JS ¶188].

129. The attachment also specified that there were two instances in which "[p]assword requirements were not met (Access)," three instances of "[l]ack of access approval prior to provisioning (Access)," and two instances of "[l]ack of independent reviewer (Access)." [SEC Ex. 28 [SW-SEC00388330-8332], at PDF page *4].

130. The attachment further detailed two SolarWinds systems as not meeting password requirements because "maximum password age is not configured as required, nor is... a password history requirement." [SEC Ex. 28 [SW-SEC00388330-8332], at PDF page *5].

131. For another control where Brown was the owner, the deficiency included that "logical access rights were not removed in a timely manner for 4 terminated users." SEC Ex. 28 [SW-SEC00388330-8332], at PDF page *5].

132. INTENTIONALLY OMITTED.

133. SolarWinds' March 3, 2020 Quarterly Risk Review, which was drafted with input from Brown, also summarized the FY2019 SOX audit summary. [SEC Ex. 8 [SW-SEC00001608-1634], at -1618]; SEC Ex. 2 [Brown Dep.] 232:22-233:25].

134. This slide also identified 27 "total control deficiencies" in the category of "IT General Controls," and it stated that 10 of the 27 control deficiencies were "not remediated" as of the time of the presentation on March 3, 2020. [SEC Ex. 8 [SW-SEC00001608-1634], at -1618].

iii. Internal FY2020 Audit Assisted by KPMG

135. Following the SUNBURST incident, SolarWinds conducted an internal audit with auditors from KPMG concerning the company's internal controls over financial reporting

("ICFR") in light of the SUNBURST incident. [SEC Ex. 29 [SW-SEC00648038-8052], at -8038].

136. The memorandum in SEC Ex. 29 is dated February 23, 2020, but based on context that date appears to be a typographical error, and the memorandum was prepared in February 2021 regarding the prior fiscal year. [SEC Ex. 29 [SW-SEC00648038-8052], at -8038].

137. A memorandum prepared by "Internal Audit/KPMG" and titled "Evaluation of ITGC Deficiencies," assessed "the severity of the [SolarWinds] [information technology] general control deficiencies" as they related to SolarWinds' ICFR during the period ending December 31, 2020. [SEC Ex. 29 [SW-SEC00648038-8052], at -8038].

138. The memorandum was reviewed by Chief Financial Officer Bart Kalsu. [SEC Ex. 29 [SW-SEC00648038-8052], at -8038].

139. The memorandum documented the conclusions of SolarWinds' management regarding these issues. [SEC Ex. 29 [SW-SEC00648038-8052], at -8038].

140. SolarWinds' identified two of the same design deficiencies also flagged in the PwC external audit (*see infra*). [SEC Ex. 29 [SW-SEC00648038-8052], at -8038; SEC Ex. 30 [PWC-SEC-00041801-1860], at -1836].

141. The first such identified design deficiency was a "[l]ack of adequate preventative and/or detective authentication controls over domain administrator accounts to restrict access to financial reporting infrastructures to only approved and authorized users." [SEC Ex. 29 [SW-SEC00648038-8052], at -8038].

142. The second such identified design deficiency was a "[l]ack of adequate preventative and/or detective authentication controls over user accounts to restrict access to financial

reporting systems to only approved and authorized users." [SEC Ex. 29 [SW-SEC00648038-8052], at -8038].

143. The memorandum contained a section entitled "Material Weakness Considerations." [SEC Ex. 29 [SW-SEC00648038-8052], at -8042].

144. That section evaluated several factors that can affect the severity of a control deficiency. [SEC Ex. 29 [SW-SEC00648038-8052], at -8042].

145. That section ended with the following statement: "Based on our assessment of the ineffective [information technology general controls] related to the cyber incident discussed [above], we assess that these controls rise to the level of significant deficiency." [SEC Ex. 29 [SW-SEC00648038-8052], at -8042].

146. This memorandum also noted that SolarWinds' internal audit had "identified 8 deficiencies related to ITGC operating effectiveness and 3 deficiencies related to design effectiveness." [SEC Ex. 29 [SW-SEC00648038-8052], at -8042].

147. The memorandum also noted management's conclusion that one of those design deficiencies, a "[l]ack of adequate preventative and/or detective controls over generic accounts to restrict access to financial reporting systems to only approved and authorized users," should be aggregated with the other deficiencies described in the memorandum. [SEC Ex. 29 [SW-SEC00648038-8052], at -8042].

148. The "Overall Conclusion" of that memorandum was that "[m]anagement concluded that an internal control ***significant deficiency*** exists in aggregate for 1) authentication and 2) management of generic accounts, and therefore merits attention by those charged with oversight of the company's financial reporting." [SEC Ex. 29 [SW-SEC00648038-8052], at -8043 (emphasis in original)].

iv. External FY2020 Audit by PwC

149. An external SOX audit was conducted by PricewaterhouseCoopers ("PwC") for Fiscal Year 2020. [SEC Ex. 52 [Johnson Dep.] 251:6-22; SEC Ex. 30 [PWC-SEC-00041801-1860]; SEC Ex. 71 [PWC-SEC-00046944-6969]].

150. In that audit, as documented in a February 19, 2021 memorandum, PwC examined SolarWinds' internal controls in Fiscal Year 2020, including whether there were significant deficiencies as a result of the aggregation of certain IT-related deficiencies. [SEC Ex. 30 [PWC-SEC-00041801-1860], at -1836].

151. Upon completion of the 2020 SOX audit, PwC identified design deficiencies in SolarWinds' IT general controls during the 2020 fiscal year. [SEC Ex. 30 [PWC-SEC-00041801-1860], at -1836; SEC Ex. 84 [SW-SEC00550676-0722], at -0693].

152. The design deficiencies identified by PwC were (i) a "[l]ack of adequate preventative and/or detective authentication controls over domain administrator accounts to restrict financial reporting infrastructure access to only approved and authorized users," (ii) a "[l]ack of adequate preventative and/or detective controls over generic accounts to restrict financial reporting systems access to only approved and authorized users," and (iii) a "[l]ack of adequate preventative and/or detective authentication controls over user accounts to restrict access to financial reporting systems to only approved and authorized users." [SEC Ex. 30 [PWC-SEC-00041801-1860], at -1836; SEC Ex. 84 [SW-SEC00550676-0722], at -0693].

153. PwC concluded that these deficiencies aggregated to a significant deficiency. [SEC Ex. 30 [PWC-SEC-00041801-1860], at -1836].

154. PwC communicated this significant deficiency conclusion to SolarWinds' management, and to SolarWinds' audit committee, in February 2021. [SEC Ex. 30 [PWC-

SEC-00041801-1860]; SEC Ex. 71 [PWC-SEC-00046944-6969]; SEC Ex. 72 [PWC-SEC-00047455-7458]].[6]

155. PwC concluded that this significant deficiency remained unremediated as of December 31, 2020, and communicated this to SolarWinds' audit committee. [SEC Ex. 84 [SW-SEC00550676-0722], at -0693].

156. PwC communicated this significant deficiency conclusion to SolarWinds' management, and to SolarWinds' audit committee, in February 2021. [SEC Ex. 30 [PWC-SEC-00041801-1860]; SEC Ex. 71 [PWC-SEC-00046944-6969]; SEC Ex. 72 [PWC-SEC-00047455-7458]].

V. SOLARWINDS' INTERNAL DESCRIPTIONS OF SOLARWINDS' PASSWORD CONTROLS WERE INCONSISTENT WITH THE SECURITY STATEMENT.

157. The Security Statement described SolarWinds' purported Authentication and Authorization practices, including password practices as the following:

> We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha and

[6] The parties' Joint Statement of Undisputed Facts [ECF No. 166] contains the statement that "[u]pon completion of the 2019 and 2020 SOX audits, PwC did not identify any material weakness or significant deficiency with respect to these controls," referring to SolarWinds' IT general controls [JS ¶103]. As described above, PwC identified design deficiencies that aggregated to a finding of a "significant deficiency" in its 2020 SOX audit, which PwC communicated to the company's management and audit committee. Paragraph 103 of the Joint Statement is incorrect insofar as it suggests that PwC did not identify a significant deficiency with respect to SolarWinds' 2020 SOX audit. The SEC asserts this language was the result of an error during the drafting process in which the SEC only intended to agree that no significant deficiency was disclosed. The SEC proposed a correction to Defendants' counsel to correspond with the documentary record on this issue prior to today's filing, however defense counsel takes the position that the Joint Statement of Undisputed Facts is binding. Although the SEC regrets this error, and apologizes for any inconvenience it causes the Court, the source documents plainly reveal that there was in fact a significant deficiency identified by PwC in the 2020 SOX audit. [*See* SEC Ex. 30 [PWC-SEC-00041801-1860], at -1836, -1848, -1850-51].

numeric characters, which are deployed to protect against unauthorized use of passwords. Passwords are individually salted and hashed. [Ex. A to JS at 3].

158. SolarWinds' password policy was important to its business because, if enforced, it served to prevent negative consequences that could come from unauthorized access, such as stealing data or the unauthorized sharing of information. [SEC Ex. 54 [Thompson Dep.] 107:6-109:25].

159. Kevin Thompson, SolarWinds' CEO at the time, recognized that cybersecurity incidents such as hackings and unauthorized access could have a negative impact on SolarWinds, such as a loss of business or reputational damage. [SEC Ex. 54 [Thompson Dep.] 108:7-110:3, 263:15-19 (marking SolarWinds Form S-1), 287:8-17, 289:25-290:20, 293:23-297:6].

160. Among other things, SolarWinds' password policy included specific password complexity requirements, including that: (1) passwords must be at least 8 characters in length; (2) passwords must contain characters from three of the following four categories: (a) English uppercase characters (A through Z), (b) English lowercase characters (a through z), (c) Base 10 digits (0 through 9), and (d) Non-alphabetic characters (for example, !, $, #, %). [JS ¶113; SEC Ex. 31 [SW-SEC00012332-2343], at -2336].

A. SolarWinds' Password Complexity Requirements Were Not Enforced on All Applicable Systems.

i. solarwinds123 password incident

161. In November 2019, an outside security researcher notified SolarWinds that "[he had] found a public Github repo which is leaking ftp credential [that] belongs to SolarWinds." [SEC Ex. 35 [SW-SEC00001464]; JS ¶187].

162. The credentials were for an Akamai server used by SolarWinds to distribute downloads of its products to its customers. [SEC Ex. 35 [SW-SEC00001464]; SEC Ex. 36 [Quitugua Inv. Vol II] 358:22-359:19].

163. The researcher explained that, with those credentials, "any hacker could upload malicious exe and update it with release [of] SolarWinds product." [SEC Ex. 35 [SW-SEC00001464]].

164. Mr. Quitugua confirmed in his SEC investigative testimony that with this password, "anybody could upload executables to the...Akamai [server]." [SEC Ex. 36 [Quitugua Inv. Vol. II] 360:5-15].

165. The password was "solarwinds123," which was described by Mr. Quitugua and Brown as a "very weak" password. [JS ¶187; SEC Ex. 34 [SW-SEC00407702-7707], at -7702; SEC Ex. 36 [Quitugua Inv. Vol. II] 360:16-361:25].

166. Mr. Quitugua also described it as a non-complex password. [JS ¶187; SEC Ex. 36 [Quitugua Inv. Vol. II] 360:16-361:25].

167. The password did not comply with SolarWinds' password complexity requirements. [SEC Ex. 36 [Quitugua Inv. Vol. II] 360:16-361:25; JS ¶113; *see also* Ex. 1 to Graff Decl. [Graff Rep.] ¶¶86-93] (explaining the problems with the "solarwinds123" incident and how this incident was inconsistent with the Security Statement)].

168. Brown confirmed the researcher's description in a December 2020 email, saying: "With that credential they could upload anything to downloads.solarwinds.com. I have assumed this was our main download site.... The point they were making was that they could have corrupted one our downloads. Replacing files or corrupting what was present in our download site. This was managed and resolved quickly but it did take place and a very weak

password existed to access that environment." [SEC Ex. 34 [SW-SEC00407702-7707], at -7702].

169. The InfoSec team recognized that the use of such a weak password was not definitively a one-time occurrence. Mr. Quitugua explained that, "There may have been the possibility that in the lab environments…weak passwords [such as 'solarwinds123'] were in use." [SEC Ex. 36 [Quitugua Inv. Vol. II] 362:1-363:17].

170. Dr. Rattray's report does not mention Lee Zimmerman. [SEC Ex. 47 [Rattray Rep.], *passim*].

ii. Additional password problems[7]

171. The June, August, and September 2019 FedRAMP Spreadsheets prepared by Ms. Pierce contained several findings relating to password deficiencies. [SEC Ex. 22 [SW-SEC00151673-1675]; SEC Ex. 23 [SW-SEC00045356-5358]; SEC Ex. 24 [SW-SEC00218068-8069]; *see also* SEC Ex. 23 [SW-SEC00045356-5358], at PDF page *5 ("The security controls and enhancements have been selected from the NIST SP 800-53 Revision 4 catalog of controls.")].

172. Although Ms. Pierce had no technical responsibility for the password policy, for purposes of preparing the spreadsheet she coordinated with both employees with technical experience and with Brown on the password policy as part of SolarWinds' annual review requirement. [SEC Ex. 63 [Pierce Dep.] 23:15-24:19].

[7] Some of the evidence cited in support of SolarWinds' access controls deficiencies in Section IV, *supra*, is also evidence of SolarWinds repeatedly failing to comply with its own password policy.

173. A September 2019 email from Ms. Pierce to Ms. Johnson and Brown related to a security risk assessment conducted by engineers working on a SolarWinds application called SWICUS, [SEC Ex. 63 [Pierce Dep.] 88:1-95:5]], observed that "Passwords have no specific parameters, as stated in the IT guidelines"; and "Passwords are able to be reused and are not changed at a set number of days." [SEC Ex. 37 [SW-SEC00151471-1473], at -1471 and PDF page *5].

174. A SolarWinds March 3, 2020 Quarterly Risk Review that was drafted with input from Brown and shared with SolarWinds' CIO, who in turn updated SolarWinds' CTO, CFO, and General Counsel, summarized the FY2019 SOX audit summary. [SEC Ex. 2 [Brown Dep.] 187:5-188:14, 233:5-25; SEC Ex. 52 [Johnson Dep.] 209:15-211:9; SEC Ex. 8 [SW-SEC00001608-1634], at -1618].

175. In a slide titled "SOX/To Be Remediated (IT Controls)," the Quarterly Risk Review presentation included that "[p]assword requirements [were] not met" and various deficiencies related to "user access." [SEC Ex. 8 [SW-SEC00001608-1634], at –1620; *see also* SEC Ex. 28 [SW-SEC00388330-8332], at -8330].

B. Failures of Password Policy for Shared Accounts

176. In a different version of the March Major Project Portfolio, which was revised on or about March 15, 2018, it acknowledged the "[u]se of shared accounts throughout internal and external applications." [SEC Ex. 32 [SW-SEC00012265-2275], at -2268].

177. This presentation also contained an action item to "Work with teams to decommission use of shared accounts." [SEC Ex. 32 [SW-SEC00012265-2275], at -2268; *see also* Ex. 1 to

Graff Decl. [Graff Rep.] ¶¶117-123 (explaining the problems with shared accounts and how they deviate from the Security Statement)].

178. Over one year later, in a May 17, 2019 Security & Compliance Program Quarterly Review, it stated that SolarWinds had an ongoing project to remedy "Use of shared accounts throughout internal and external applications." [SEC Ex. 21 [SW-SEC00001635-1652], at -1644].

179. That presentation also contained an action item to "Work with teams to decommission use of shared accounts." [SEC Ex. 21 [SW-SEC00001635-1652], at –1644. *See also* ¶¶26-27, 31-32, *supra* (April 2018 audit results stated that "[s]hared SQL legacy account login credentials [were] used" for three business units)].

C. Contrary to the Security Statement, SolarWinds Passwords Were Not Consistently Maintained in an Encrypted State.

180. In addition to the password complexity requirements, the Security statement also specified that "Passwords are individually salted and hashed." [Ex. A to JS at 3].

181. The phrase "salted and hashed" means that when a user logs into his or her computer, he or she "would be logging into [his or her] active directory account," which encrypts the password with a key. [SEC Ex. 2 [Brown Dep.] 116:5-117:18; SEC Ex. 64 [Griffiths Dep.] 84:20-85:14].

182. An April 2018 SolarWinds audit found database passwords that were "not encrypted within the configuration file," login credentials that were "stored in plain text in configuration files," and passwords that were "stored in plain text on the public web server in the web configuration file and in the system registry of the machine" [SEC Ex. 33 [SW- SEC00043080-3084], at -3080-3082].

183. The April 2018 audit finding meant that the referenced passwords were not "individually salted and hashed." [SEC Ex. 2 [Brown Dep.] 117:4-11; SEC Ex. 64 [Griffiths Dep.] 84:20-85:14; SEC Ex. 33 [SW- SEC00043080-3084], at -3082].

VI. SOLARWINDS' INTERNAL DESCRIPTIONS OF SOLARWINDS' SECURE DEVELOPMENT LIFECYCLE WERE INCONSISTENT WITH THE SECURITY STATEMENT.

184. The Security Statement described SolarWinds' purported Secure Development Lifecycle as the following:

> **Software Development Lifecycle**
>
> We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities.
>
> Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments. The SolarWinds architecture teams review our development methodology regularly to incorporate evolving security awareness, industry practices and to measure its effectiveness.

[Ex. A to JS at 3].

185. The term "secure development lifecycle" generally refers to "a set of practices that support security assurance and compliance requirements." [https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices (last visited June 13, 2025)].

186. Microsoft's publicly available description of an SDL (a process Microsoft created) indicates that threat modeling is an inherent part of it. [https://www.microsoft.com/en-us/securityengineering/sdl/practices (last visited June 13, 2025) (outlining steps of the SDL, including "3. Perform security design review and threat modeling.")].

187. Threat modeling is a standard part of an SDL. [https://www.microsoft.com/en-us/securityengineering/sdl/practices (last visited June 13, 2025) (outlining steps of the SDL, including "3. Perform security design review and threat modeling."); *see also* Ex. 1 to Graff Decl. [Graff Rep.] ¶¶147, 185 and materials cited therein (describing threat modeling as part of the SDL)].

A. SolarWinds Did Not Conduct the Amount or Type of Testing Described in the Security Statement.

188. A December 2018 Security Operations Summary included a slide titled "Security Projects: Key Areas to Address Gaps in Information Security." On that slide, the following "Gap Analysis" was part of the "Security & SSDLC" "Focus Area" that was highlighted in yellow: "Integrate and formalize security best practices into existing secure development lifecycle." [SEC Ex. 20 [SW-SEC00638663-8677], at -8674].

189. The same slide further noted for the focus area "Security Awareness Training" (again highlighted in yellow) that the gap analysis was: "Establish a formal program to educate users on the importance of protecting SolarWinds information and information systems." [SEC Ex. 20 [SW-SEC00638663-8677], at -8674].

190. The May 17, 2019 Security & Compliance Program Quarterly had a slide titled "Security & Compliance Initiatives." Under the initiative "Secure Development Lifecycle," it stated: "Working with the engineering and development teams to continue to mature and adopt the SDL." [SEC Ex. 21 [SW-SEC00001635-1652], at -1641].

191. The March 3, 2020 Quarterly Risk Review discussed the need to "[i]ncrease SDL adoption" and "[e]xpand [the] pen testing program" at SolarWinds. [JS ¶197; SEC Ex. 8 [SW-SEC00001608-1634], at -1611, -1613].

192. In October 2020, the Q4 2020 Quarterly Risk Review discussed the need to "[i]ncrease SDL awareness and adoption." [SEC Ex. 9 [SW-SEC00001582-1601], at -1587].

193. As per Kevin Thompson, SolarWinds made numerous acquisitions of other software companies, which made implementation of secure development lifecycle a "continuous effort." [SEC Ex. 54 [Thompson Dep.] 172:6-175:13].

194. In 2019, there were many instances in which customers conducted their own penetration testing and found vulnerabilities that SolarWinds had not caught internally. [SEC Ex. 64 [Griffiths Dep.] 42:17-51:9].

195. Mr. Griffiths explained such instances in his deposition:

> Q. [D]o you recall any instances where customers did their own pen testing, identified a vulnerability, sent it to you, you sent it over to the engineering team for validation and they validated that there was, indeed, a vulnerability?
>
> A. Yes.…I can't recall specific examples. There was a lot. There was many over the period of time.…[They would have begun in] 2019 maybe.…
>
> Q. [D]o you recall any instances where a customer uncovered one of these vulnerabilities and people inside SolarWinds expressed concern that this is something we should have uncovered ourselves with our own pen testing?
>
> A. I don't recall any specifics, but it's -- it's possible.

[SEC Ex. 64 [Griffiths Dep.] 42:17-43:16, 50:19-51:1].

196. A July 10, 2020 PM Security Vulnerability & Incident Review, prepared by Brown and reviewed by Ms. Johnson, stated on a slide titled "ITOM Core Highlights and Asks": "Customers continue to actively engage 3rd party penetration testers as part of their compliance efforts." [SE97C Ex. 50 [SW-SEC00006628-6648], at -6635; SEC Ex. 19 [Bliss Dep.] 265:7-266:23].

197. The presentation also warned that "[i]nconsistent internal security testing as part of product final security reviews don't always include web application testing before release." [SEC Ex. 50 [SW-SEC00006628-6648], at -6635; SEC Ex. 19 [Bliss Dep.] 264:4-265:6].

B. SolarWinds Did Not Conduct Threat Modeling—an Essential SDL Process.

198. "Threat modeling" or "threat analysis" is "'the process of examining who is likely to attack a system and how they are likely to attack it.'" [Ex. 1 to Graff Decl. [Graff Rep.], at 78 n. 263 (quoting Graff and Van Wyk (2003) Secure Coding: Principles and Practices, p. 144)].

199. Undertaking a threat analysis is advisable because, among other things, it "'help[s] during the design and implementation of the application by guiding the designer on what defenses to put in place to protect the application.'" [Ex. 1 to Graff Decl. [Graff Rep.], at 78 n. 263 (quoting Graff and Van Wyk (2003) Secure Coding: Principles and Practices, p. 144)].

200. Mr. Kim explained that threat modeling between products "was not standardized across the different parts of the organization." [SEC Ex. 43 [Kim Dep.] 148:8-24].

201. A SolarWinds May 17, 2019 Security & Compliance Program Quarterly Review noted that, "Project to operationalize and improve overall security for SolarWinds. This effort includes training (security and SDL), department plans for addressing security, KPIs, and an annual audit to measure the effectiveness of security practices within SolarWinds." [JS ¶194; [SEC Ex. 21 [SW-SEC00001635-1651], at -1650].

202. In the June FedRAMP Assessment prepared by Ms. Pierce, described above, for the topic "The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as built system, component, or service," Ms. Pierce's comment was, "Program in the works." [SEC Ex. 22 [SW-SEC00151673-1675], at PDF page *9, line 264].

203. A July 2019 security evaluation, by Stas Starikevich and Wojciech Pitera, of MSP "key products – RMM, NCentral, and Backup" stated that "each product seems to have its own ways of marking security issues that do not follow recently established SW standards" and "[n]o threat modeling nor analysis is performed as part of any process (except MSP Backup Engineering)." [JS ¶195; SEC Ex. 45 [SW-SEC00166790-6799], at -6794; SEC Ex. 19 [Bliss Dep.] 271:8-17, 276:5-14, 277:24-278:8].

204. When asked about the purpose of the July 2019 security evaluation, Mr. Bliss, SolarWinds' designated Rule 30(b)(6) representative, testified that he did not know. [SEC Ex. 19 [Bliss Dep.] 271:1-2].

205. When asked about the July 2019 security evaluation and why SolarWinds was performing an analysis pursuant to the NIST security framework, Mr. Bliss testified that he did not know. [SEC Ex. 19 [Bliss Dep.] 271:18-272:6].

206. When asked about the July 2019 security evaluation and whether an assessment of the NIST security framework was done on a regular basis, Mr. Bliss testified that he did not know. [SEC Ex. 19 [Bliss Dep.] 271:18-272-15].

207. When asked about the July 2019 security evaluation's reference to "[d]esign documentation overall is lacking and unstructured for the majority of products," Mr. Bliss did not have an understanding of the basis of this sentence. [SEC Ex. 19 [Bliss Dep.] 272:24-273:6].

208. When asked about the July 2019 security evaluation's reference to "These are crucial for threat modeling and other security activities of the SSDLC," Mr. Bliss did not have an understanding of the precise basis of the statement. [SEC Ex. 19 [Bliss Dep.] 270:7-274:22].

209. In his expert report, Mr. Graff explained the importance of developing the OIP under an SDL. [Ex. 1 to Graff Decl. [Graff Rep.] ¶¶163-183].

210. The Security Statement did not specify that the SDL applied only to products sold to customers, but not to internal software that SolarWinds used to support and manage these same products. [Ex. 1 to Graff Decl. [Graff Rep.] ¶164].

211. The August 16, 2019 Security & Compliance Program Quarterly Overview discussed the "Secure Software Development Lifecycle (SSDL)." [SEC Ex. 70 [SW-SEC00264310-4364], at -4320].

212. The SSDL category received a NIST Maturity Level of "2" for the objective "[e]mployees are aware of an[d] utilize a security software development lifecycle in their day to day activities." [SEC Ex. 70 [SW-SEC00264310-4364], at -4320].

213. The legend in the presentation defined a NIST Maturity Level of "2" as "[t]he organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance." [SEC Ex. 70 [SW-SEC00264310-4364], at -4319].

214. As Mr. Kim testified, a NIST Maturity Level of "2" for this objective was accurate. [SEC Ex. 70 [SW-SEC00264310-4364]. at -4319, -4320]; SEC Ex. 43 [Kim Dep.] 252:5-253:2].

C. SolarWinds Did Not Maintain Separate Development and Production Environments as Described in the Security Statement.

215. SolarWinds' Security Statement also asserted that "SolarWinds maintains separate development and production environments." [Ex. A to JS at 2].

216. It is standard security practice to separate development and production environments to reduce the risks of unauthorized access. [Ex. 1 to Graff Decl. [Graff Rep.], at ¶ 151 n. 290

(citing ISO/IEC 27001:2013(E), A.12.1.4. ("Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.") and NIST Cybersecurity Framework at p. 33. ("PR.DS-7: The development and testing environment(s) are separate from the production environment.")); SEC Ex. 47 [Rattray Rep.] ¶186; SEC Ex. 36 [Quitugua Inv. Vol. I] 134:9-17 ("Q From a security standpoint, is it important for the development staging, testing, [quality assurance], and production environment to be separated? A Yes. Q Why? A So that any changes within the development and staging environments don't affect production systems that could potentially bring down and make them unavailable for -- for the services that they provide.")].

217. As of at least November 2019, SolarWinds "developers were working inside the production environment." [SEC Ex. 47 [Rattray Rep.] ¶190; *see also* SEC Ex. 65 [SW-SEC00168778-8780], at -8780 tab '7.13.2020 Review', cell C9 ("Developers have write access to production Backup data as part of their permission set. They are using the API's just to pull data for usage billing but those (3) API's have write permissions which are not used or needed."); SEC Ex. 46 [SW-SEC00254254-4266], at -4265 ("The developers are developing in Production as the staging/dev environments are not suitable.")].

218. This meant that SolarWinds did not have separate development and production environments. [SEC Ex. 47 [Rattray Rep.] ¶190; *see also* SEC Ex. 65 [SW-SEC00168778-8780], at -8780, tab '7.13.2020 Review', cell C9; SEC Ex. 46 [SW-SEC00254254-4266], at -4257, -4265; Ex. 1 to Graff Decl. [Graff Rep.] ¶¶150-162].

219. Chris Day, VP of Global DevOps and Technology Operations, described this situation as the following: "highlighted item [The developers are developing in Production] needs to stop immediately. Under no circumstances is development to be done in production.… That is

a significant security and Sox [sic] violation. As part of our ISO it also need to be filed as a non-conformity and reported." He then added: "This is a separation of duties and a control issue that needs to be decided between Tim O, Rani, and Tim Brown. It is clearly bad – violation of SOX controls and an ISO violation that we will need to register as there is no separate [sic] of duties and developers have full access to a billing environment (which we need to file regardless as it already exists)." [SEC Ex. 46 [SW-SEC00254254-4266], at -4257, -4265].

220. This incident was in fact a significant security violation. [SEC Ex. 46 [SW-SEC00254254-4266], at -4257, -4265; *see also* Ex. 1 to Graff Decl. [Graff Rep.] ¶¶150-162].

221. When questioned about this practice by his superiors, a Senior Product Manager responded that "it's not something new, we were developing billing using production services since the beginning as only production has data to test billing." [SEC Ex. 46 [SW-SEC00254254–2466], at -4264, -4265].

222. The risk from this lack of separation was raised to Brown, who thereafter stated that a risk acceptance form should be filed. [SEC Ex. 46 [SW-SEC00254254-4266], at -4256 (Brown stating, "We should not disrupt business, we should file a RAF accept risk for a period of time so that we can develop the correct approach.")]. SolarWinds thereafter continued to leave this issue unaddressed for months, even well after the date by which Brown had said it should be resolved. [Ex. 1 to Graff Decl. [Graff Rep.] ¶¶150-162].

223. Risk acceptance forms or RAFs were a means for SolarWinds to go outside of its "standard process" and document the approval of letting the risk posed by a problem in the software development process persist by submitting a RAF for review and approval by the SolarWinds executive (Vice President or higher) responsible for the asset or service accepting

the risk. Brown was one such reviewer. [SEC Ex. 2 [Brown Dep.] 105:16-106:24; *see also* SEC Ex. 25 [Quitugua Dep.] 210:11-23; SEC Ex. 81 [SW-SEC00168009-0017], at -0011].

224. Additionally, as per Mr. Quitugua, SolarWinds "ha[s] experienced security incidents because of errors made when accessing production data and have also had to document compliance violations because of this poor security practice." [SEC Ex. 46 [SW-SEC00254254–4266], at -4260].

VII. SOLARWINDS' CLAIM IN THE SECURITY STATEMENT THAT IT FOLLOWS THE NIST CYBERSECURITY FRAMEWORK OMITTED INFORMATION ABOUT THE COMPANY'S PERVASIVELY LOW SCORES ON INTERNAL NIST ASSESSMENTS.

225. The Security Statement described SolarWinds' purported compliance with the NIST Cybersecurity Framework ("NIST Framework"): "SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect and respond to security incidents." [Ex. A to JS at 3].[8]

A. SolarWinds Used Scorecards and Spreadsheets to Assess Its Progress Toward NIST Compliance.

226. The NIST scorecards assessed the state of SolarWinds' cybersecurity program. [SEC Ex. 19 [Bliss Dep.] 190:19-191:10].

i. 2017 NIST scoring measures

227. SolarWinds tracked maturity levels on the NIST Framework before it started presenting the "NIST Scorecards" to SolarWinds' senior executives. [SEC Ex. 19 [Bliss Dep.] 86:16-24].

[8] The evidence cited above about the other specific cybersecurity failings is also evidence that SolarWinds claim to follow NIST was materially misleading.

228. Mr. Quitugua began looking at the NIST Framework in early 2017. [SEC Ex. 19 [Bliss Dep.] 86:21-24].

229. As Mr. Thompson said at his deposition, NIST was a "security maturity model...that we were using to grade ourselves against in terms of the maturity of our security environment." [SEC Ex. 54 [Thompson Dep.] 156:4-11]. By "maturity," Thompson meant "how advanced are the controls, how automated are the controls." [SEC Ex. 54 [Thompson Dep.] 157:6-15].

230. On August 9, 2017, Mr. Quitugua emailed Brown with the subject line "SWI Security Program Assessment." [SEC Ex. 1 [SW-SEC00350067-0069], at -0067]. Mr. Quitugua stated: "Here is my assessment of the state of our security program here at SWI with my assessment based on the CIS top 20 critical security controls mapped to the NIST Cybersecurity framework." [SEC Ex. 1 [SW-SEC00350067-0069], at -0067].

231. Mr. Quitugua created the attachment to his email—a scorecard of the NIST maturity levels—shortly after Brown joined SolarWinds in order to give Brown a "baseline of current state of my own personal assessment of the organization in terms of security control." [SEC Ex. 25 [Quitugua Dep.] 192:14-23].

232. As part of his work creating the scorecard of the NIST maturity levels attached to his August 9, 2017 email, Mr. Quitugua testified that he "took the CIS security controls, the top 20 critical controls, and made an attempt to map it to the NIST cybersecurity framework." [SEC Ex. 25 [Quitugua Dep.] 194:6-12].

233. August 2017 was the first time a scorecard of the NIST maturity levels had been prepared at SolarWinds. [SEC Ex. 25 [Quitugua Dep.] 195:7-10].

234. One of the slides in the attachment to Mr. Quitugua's August 9, 2017 email contained a spreadsheet that included "Function[s]," "Categor[ies]," and "Maturity Level" scores. [SEC Ex. 1 [SW-SEC00350067-0069], at PDF page *5].

235. In his deposition, Mr. Quitugua explained that he prepared this slide and the categories were "CIS controls" mapped "to the NIST cybersecurity framework." [SEC Ex. 25 [Quitugua Dep.] 194:13-195:2, 195:11-18; SEC Ex. 1 [SW-SEC00350067-0069], at PDF page *5].

236. In the legend on this slide, a score of "0" meant "[t]here is no evidence of the organization meeting the security control objectives or is unassessed." [SEC Ex. 1 [SW-SEC00350067-0069], at PDF page *5]. A score of "1" meant "[t]he organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives." [SEC Ex. 1 [SW-SEC00350067-0069], at PDF page *5]. A score of "2" meant "[t]he organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance." [SEC Ex. 1 [SW-SEC00350067-0069], at PDF page *5]. A score of "3" meant "[t]he organization has a documented, detailed approach to meeting the security control objectives, and regularly measures its compliance." [SEC Ex. 1 [SW-SEC00350067-0069], at PDF page *5].

237. This same slide in the attachment to the August 9, 2017 email contained a spreadsheet of "Functions," "Categor[ies]," and "Maturity Level" scores, [SEC Ex. 1 [SW-SEC00350067-0069], at PDF page *5], it had the following findings:

				Organization		
	Function	Category	CSC Top 20 Controls	CorelT	MSP	Monitoring Cloud
Governance	Identify	Asset Management	1, 2	2	2	0
		Business Environment	-	0	0	0
		Risk Assessment	-	1	1	0
		Governance	4	2	2	1
	Protect	Risk Management Strategy	-	2	1	1
		Access Control	5, 9, 11, 12, 13, 14, 15, 16	2	2	1
		Awareness and Training	5, 17	1	1	0
		Data Security	1, 2	1	1	1
		Information Protection Processes and Procedures	3, 4, 7, 9, 10, 11, 18, 19	2	1	1
		Maintenance	3, 4, 5, 11, 12	2	2	0
		Protective Technology	5, 6, 7, 8, 11, 13, 14, 16	2	2	1
	Detect	Anomalies and Events	6, 9, 12, 19	2	2	0
		Security Continuous Monitoring	4, 8, 16, 19	3	3	0
		Detection Processes	19	3	3	3
	Respond	Response Planning	19	4	4	4
		Communications	19	4	4	4
		Analysis	6, 19	3	3	3
		Mitigation	4, 19	3	3	3
		Improvements	19, 20	3	3	3
	Recover	Recovery Planning	10	2	2	2
		Improvements	20	2	2	2
		Communications	-	2	2	2

[SEC Ex. 1 [SW-SEC00350067-0069], at PDF page *5].

ii. 2018 NIST scoring measures

238. Mr. Quitugua was the "DOIT lead" for the slide titled "Security Assessment and Remediation" of the March 2018 Major Project Portfolio. [SEC Ex. 25 [Quitugua Dep.] 200:21-201:4, 208:20-24; SEC Ex. 14 [SW-SEC00042892-2964], at -2906].

239. That slide stated, "Need to identify security controls that don't already map to NIST framework." [SEC Ex. 25 [Quitugua Dep.] 208:20-24; SEC Ex. 14 [SW-SEC00042892-2964], at -2906].

240. Mr. Quitugua confirmed that in the process of preparing this slide, "there were some areas where [he] personally did not observe the control being implemented…so it's reasonable also to expect that we would establish baselines for those areas that were unobserved." [SEC Ex. 25 [Quitugua Dep.] 206:8-21].

241. Just weeks before SolarWinds' IPO, on October 1, 2018, Mr. Quitugua emailed another spreadsheet assessing "Function[s]," "Categor[ies]," and "Maturity evel" scores. [SEC Ex. 4 [SW-SEC00013676-3678], at PDF page *5].

242. The legend was the same as the August 2017 version. [*Compare* SEC Ex. 4 [SW-SEC00013676-3678], at PDF page *5, *with* SEC Ex. 1 [SW-SEC00350067-0069], at PDF page *5].

[REMAINDER OF PAGE INTENTIONALLY BLANK]

243. This slide contained the following findings:

				Organization		
	Function	Category	CSC Top 20 Controls	CoreIT	MSP	Cloud
Cybersecurity Framework	Identify	Asset Management	1, 2	2	2	2
		Business Environment	-	3	3	2
		Risk Assessment	-	3	3	1
		Governance	4	3	3	1
		Risk Management Strategy	-	3	3	1
	Protect	Access Control	5, 9, 11, 12, 13, 14, 15, 16	2	2	2
		Awareness and Training	5, 17	1	1	1
		Data Security	1, 2	2	2	1
		Information Protection Processes and Procedures	3, 4, 7, 9, 10, 11, 18, 19	3	3	1
		Maintenance	3, 4, 5, 11, 12	3	3	0
		Protective Technology	5, 6, 7, 8, 11, 13, 14, 16	2	2	1
	Detect	Anomalies and Events	6, 9, 12, 19	3	3	1
		Security Continuous Monitoring	4, 8, 16, 19	3	2	0
		Detection Processes	19	3	3	0
	Respond	Response Planning	19	4	4	4
		Communications	19	4	4	4
		Analysis	6, 19	3	3	3
		Mitigation	4, 19	3	3	3
		Improvements	19, 20	3	3	3
	Recover	Recovery Planning	10	3	3	3
		Improvements	20	3	3	3
		Communications	-	4	4	4

[SEC Ex. 4 [SW-SEC00013676-3678], at PDF page *5].

iii. 2019 and later NIST scoring measures

244. The first time that NIST Maturity Level Scorecards were included in presentations for SolarWinds executive management was in the August 16, 2019 Security & Compliance Program Quarterly Overview. [SEC Ex. 5 [SW-SEC00001497-1550], at -1498, -1504, -1505; *see also* JS ¶177; SEC Ex. 19 [Bliss. Dep.] 227:5-11].

245. The "Agenda" slide of the presentation stated, "Introduce Security Score Card." [SEC Ex. 5 [SW-SEC00001497-1550], at -1498].

246. The NIST Scorecard slide in this presentation listed five security categories—"identify, protect, detect, respond, and recover"—and assigned a score to each of those categories for the years 2017 through 2019. [SEC Ex. 5 [SW-SEC00001497-1550], at -1505; *see also* JS ¶177].

247. At her deposition, Ms. Pierce testified that scores on scorecards such as this were discussed between Brown and Ms. Johnson. [SEC Ex. 63 [Pierce Dep.] 79:4-12 (identifying SEC Ex. 77 [SW-SEC00061296-1297]), 81:16-83:17].

248. As per Brown and Ms. Johnson, these scorecards were created to provide a high-level "read out to the executive team as far as [SolarWinds'] NIST CSF status" and identify areas for improvement or specific projects that were being proposed. [SEC Ex. 2 [Brown Dep.] 90:9-20; SEC Ex. 52 [Johnson Dep.] 218:19-219:1-23 ("[T]his [i.e., the NIST Scorecard] was an awareness vehicle for leadership…We created this vehicle to summarize and provide awareness to other business departments.")].

249. In the sub-rating "Secure Software Development Lifecycle (SSDL)" of this presentation, with the objective "[e]mployees are aware of an [sic] utilize a security software development lifecycle in their day to day activities," SolarWinds gave itself the NIST Maturity Level of "2." [SEC Ex. 5 [SW-SEC00001497-1550], at -1506].

250. A NIST Maturity Level of "2" meant that SolarWinds "has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance." [SEC Ex. 5 [SW-SEC00001497-1550], at -1505].

251. The second time that NIST Maturity Level Scorecards were included in presentations for SolarWinds executive management was in SolarWinds' November 15, 2019 Security &

Compliance Program Quarterly Review. [SEC Ex. 6 [SW-SEC00001551-1581], at -1576; *see also* JS ¶179].

252. On the slide titled "Protect," under the security subcategory "Authentication, Authorization, and Identity Management," with objective "[u]ser identity, authentication and authorization are in place and actively monitored across the company," SolarWinds assigned itself a NIST Maturity Level of "1." [SEC Ex. 6 [SW-SEC00001551-1581], at -1578].

253. A NIST Maturity Level of "1" is defined as "[t]he organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives." [SEC Ex. 6 [SW-SEC00001551-1581], at -1576; *see* JS ¶179].

254. The presentation also states, "Access and privilege to critical systems/data is inappropriate." [SEC Ex. 6 [SW-SEC00001551-1581], at -1578].

255. In the sub-category "Secure Software Development Lifecycle (SSDL)" of this presentation, with the objective "[e]mployees are aware of an [sic] utilize a security software development lifecycle in their day to day activities," SolarWinds gave itself the NIST Maturity Level of "2." [SEC Ex. 6 [SW-SEC00001551-1581], at -1577].

256. A NIST Maturity Level of "2" meant that SolarWinds "has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance." [SEC Ex. 6 [SW-SEC00001551-1581], at -1576].

VIII. OTHER DOCUMENTS SHOWING THAT SOLARWINDS HAD POOR CYBERSECURITY.

A. Employees Recognized Consistently Poor Cybersecurity in Internal Messages.

257. In a November 4, 2020 Instant Message ("IM") string between Ondrej Fitzek, a SolarWinds engineer, and InfoSec team member Harry Griffiths, Mr. Fitzek complained in a

series of messages that: "We filed more vulnerabilities then [sic] we fixed. And by fixed, it often means just a temporary fix…but the problem is still there and it's huge. I have no idea what we can do about it. Even if we started to hire like crazy, which we will most likely not, it will still take years. Can't really figure out how to unf**k this situation. Not good." [SEC Ex. 73 [SW-SEC00236824-6896], at -6829; SEC Ex. 64 [Griffiths Dep.] 17:1-15, 182:9-13].

258. In a November 18, 2020 IM string between Mr. Griffiths and Mr. Quitugua, Mr. Griffiths embedded a screenshot of a log of multiple vulnerabilities, and stated: "the products are riddled and obviously have been for many years with nothing being found internally like this to this extent through testing." [SEC Ex. 74 [SW-SEC00236723-6811], at -6759; SEC Ex. 78 [Griffiths Inv. Vol. II] 272:17-273:15].

259. Mr. Quitugua responded a few minutes later in a series of messages: "we're so far from being a security minded company. everytime I hear about our head geeks talking about security I want to throw up. they all live in this fantasy land smoking the same fairy dust and mushrooms." [SEC Ex. 74 [SW-SEC00236723-6811], at -6759].

260. In another November 25, 2020 message to Mr. Quitugua, Mr. Griffiths stated: "I am rolling out now. I hope you have a good time off and I will try to man the fort!" [SEC Ex. 74 [SW-SEC00236723-6811], at -6797]. Mr. Quitugua sent the following reply IM to Mr. Griffiths: "more like keep the house from burning down! lol." [SEC Ex. 74 [SW-SEC00236723-6811], at -6797]. Mr. Griffiths then responded: "hard with all these faulty electrics." [SEC Ex. 74 [SW-SEC00236723-6811], at -6797].

IX. CORRECTLY USING ACCESS CONTROLS, PASSWORD PRACTICES, AND A SECURE DEVELOPMENT LIFECYCLE WERE IMPORTANT TO SOLARWINDS' BUSINESS.

A. Internal SolarWinds Documents Show Brown and Johnson Considered Cybersecurity Practices to Be Important to SolarWinds' Business.

261. Tim Brown sent a December 14, 2017 email containing a presentation titled "Security 90 Day Review." It was a common practice when a new person joined a team at SolarWinds for them to present their findings to their supervisors. [SEC Ex. 3 [SW-SEC00262716-2743], at -2718; SEC Ex. 2 [Brown Dep.] 150:11-151:14].

262. In that presentation, Brown wrote, "Appropriate security policies, procedures, training, PEN testing are required by our commercial customers and asked for in qualifying questionnaires. Without appropriate answers we will lose business." [SEC Ex. 3 [SW-SEC00262716-2743], at -2743].

263. Rani Johnson prepared a document outlining performance goals for the second half of 2017. [SEC Ex. 26 [SW-SEC00259614-9618]; SEC Ex. 52 [Johnson Dep.] 92:4-94:1].

264. In that document she wrote: "Development Goal 1: Outline DOIT plan to sure [sic] up deficiencies that may affect IPO valuation/readiness." [SEC Ex. 26 [SW-SEC00259614-9618], at -9617].

265. Under that goal she stated: "Identified the following shortcomings that may affect IPO valuation/readiness. Work is underway to bolster by 2019." The five shortcomings identified were: (1) "Identity and Access Management"; (2) "Asset Management"; (3) "Application Sprawl"; (4) "Billing System Consolidation"; and (5) "Security Standards." [SEC Ex. 26 [SW-SEC00259614-9618], at -9617, -9618]. Ms. Johnson prepared another performance self-assessment on or about June 20, 2018. [SEC Ex. 27 [SW-SEC00302323-2334]; SEC Ex. 52 [Johnson Dep.] 112:23-115:9]. One of the goals set out in the document for Ms. Johnson was:

"Continue to improve security posture (e.g. SDL, Product Scorecards, etc.) and adoption of industry regulations (e.g. GDPR, NIST, etc.)." [SEC Ex. 27 [SW-SEC00302323-2334] at -2323, 2328; SEC Ex. 52 [Johnson Dep.] 115:12-116:13]. In the June 2018 document, she wrote: "Development Goal 1: Outline DOIT plan to sure [sic] up deficiencies that may affect IPO valuation/readiness." [SEC Ex. 27 [SW-SEC00302323-2334] at -2332; SEC Ex. 52 [Johnson Dep.] 124:5-24]. Under that goal, Ms. Johnson stated: "Identified the following shortcomings that may affect IPO valuation/readiness." [SEC Ex. 27 [SW-SEC00302323-2334] at -2332; SEC Ex. 52 [Johnson Dep.] 125:6-126:25]. The June 2018 document repeated the same five shortcomings that were identified in Ms. Johnson's 2017 performance evaluation, *see* ¶¶263-264, *supra*: (1) "Identity and Access Management"; (2) "Asset Management"; (3) "Application Sprawl"; (4) "Billing System Consolidation"; and (5) "Security Standards." [SEC Ex. 27 [SW-SEC00302323-2334] at -2332; SEC Ex. 52 [Johnson Dep.] 125:6-126:25].

B. Equity Research Analysts Following SolarWinds Considered Access Controls, Password Practices, and Secure Development Lifecycle Important to Their Recommendations.

266. Brent Thill, an equity research analyst at Jefferies, covered SolarWinds during the Relevant Period. [SEC Ex. 56 [Thill Dep.] 14:16-16:17, 30:24-31:17].

267. Matthew Hedberg, an equity research analyst at RBC, covered SolarWinds during the Relevant Period. [SEC Ex. 55 [Hedberg Dep.] 26:5-22].

268. Certain equity research analysts that covered SolarWinds and who recommended company stocks for investment during the Relevant Period, including Mr. Thill and Mr. Hedberg, considered it important that those companies follow many of the cybersecurity procedures that were detailed in the Security Statement, including role-based access controls, a secure development lifecycle, and least-privileged access. [Ex. A to JS at 2-3; SEC Ex. 56

[Thill Dep.] 43:9-15, 58:22-59:4, 60:2-5, 60:11-16, 65:11-18; SEC Ex. 55 [Hedberg Dep.] at 73:16-74:5, 120:7-121:2, 131:4-132:18].

269. For example, Mr. Thill testified that, when evaluating a software company as a potential investment, it was important to him that the company had "a comprehensive security model" in place, that the security model is "tested," and that "they haven't had any prior breaches." [SEC Ex. 56 [Thill Dep.] 41:7-21].

270. Thill also testified that "layered security is important" to him. [SEC Ex. 56 [Thill Dep.] 51:1-16].

271. Mr. Thill testified that it is "pretty important" to him, as an investment research analyst, that a software company follow a secure development lifecycle because "it's critical to ensuring the success of the software…over time." [SEC Ex. 56 [Thill Dep.] 43:9-19, 65:11-18].

272. When asked in his deposition why it was important for particular applications to be covered by the software development lifecycle, Mr. Hedberg responded, "to know that…a company's following standard practice to write code and to promote code." [SEC Ex. 55 [Hedberg Dep.] 131:4-132:18].

273. When asked in his deposition about the importance of the steps described the Security Statement's "Change Management" paragraph, Ex. A to JS at 2, Mr. Thill testified that "[i]t's really important." As Thill explained, "every change in the software process should be ensured that it's…checked…and it runs correctly." [SEC Ex. 56 [Thill Dep.] 53:1-20].

274. When asked how important the steps in the Security Statement's "Auditing and Logging" paragraph, [Ex. A to JS at 2], were to his evaluation of software companies, Mr.

Thill acknowledged that he assumed that all of the software companies that he was following employed these steps. [SEC Ex. 56 [Thill Dep.] 54:15-55:2].

275. As Mr. Thill explained, it is important for software companies "to understand who's in the system, who made the changes, why they were there, how long were they there for,…[and] you want to understand the…log of who was in the system." [SEC Ex. 56 [Thill Dep.] 54:15-23].

276. During his deposition, Mr. Hedberg testified that he would have "assumed" that SolarWinds had an audit "in place for security parameters" and that he would have wanted to know that SolarWinds' internal documents stated that least privilege access was not audited in 2019. [SEC Ex. 55 [Hedberg Dep.] 119:10-20, 120:7-11].

277. When asked how important the steps in the Security Statement's "Role-Based Access Controls" paragraph, [Ex. A to JS at 3], were to his evaluation of software companies, Mr. Thill acknowledged that they were "very important." [SEC Ex. 56 [Thill Dep.] 58:22-59:4].

278. As Mr. Thill explained, "security…is a layered model, and [role-based access controls] is one of many layers in that security model." [SEC Ex. 56 [Thill Dep.] 58:22-59:4].

279. During his deposition, Mr. Hedberg testified that he would have expected the software companies that he evaluated to engage in role-based access controls. [SEC Ex. 55 [Hedberg Dep.] 74:3-5].

280. When asked why it was important for software companies to engage in role-based access controls, Mr. Hedberg explained: "Because Employee A maybe doesn't need access to it, and it could open up a vulnerability if that employee's access is compromised and they have access to something that they shouldn't." [SEC Ex. 55 [Hedberg Dep.] 73:16-22].

281. When asked how important it was that the software companies that he evaluated have access controls set on a "least-privilege" basis, as discussed in the Security Statement, [Ex. A to JS at 3], Mr. Thill acknowledged that it was "[v]ery important" to him. As he explained, "everyone's access should have different…levels" and "[access] shouldn't be universally open to everyone." [SEC Ex. 56 [Thill Dep.] 60:2-16].

282. Mr. Thill also gave an example of the importance of role-based access controls in a company: "[Y]ou don't need the intern looking at [certain] information. You may need only the CEO looking at that information." [SEC Ex. 56 [Thill Dep.] 60:11-13].

283. Mr. Hedberg testified that he would have wanted to know that SolarWinds' internal documents stated that least privilege access was not audited in 2019 because "it could increase the risk for unauthorized access." [SEC Ex. 55 [Hedberg Dep.] 120:7-121:2].

284. Mr. Hedberg acknowledged that an "increase [in] the risk for unauthorized access" could increase the risk of a cyberattack, negatively impact the company, and reduce the company's revenue. [SEC Ex. 55 [Hedberg Dep.] 120:14-121:2].

285. Mr. Thill and Mr. Hedberg also considered it important for a software company to follow many of the procedures outlined in the Security Statement relating to user access, password best practices, and performing vulnerability and penetration testing. [Ex. A to JS at 2-3; SEC Ex. 56 [Thill Dep.] 49:8-21, 61:6-63:14, 68:17-68:21, 70:2-22; SEC Ex. 55 [Hedberg Dep.] 92:16-93:10].

286. For example, when asked how important it was that the software companies that he evaluated properly restrict administrative user access, Mr. Thill acknowledged that it was "very important" to him. As he explained, "you don't let everyone in the company have access to all data[;]" [y]ou let certain users in." [SEC Ex. 56 [Thill Dep.] 61:16-19].

287. Mr. Hedberg testified that if many employees at SolarWinds had administrator access rights beyond what they should have been authorized to have, it would be an important fact to know because it would be "potentially bad." [SEC Ex. 55 [Hedberg Dep.] 92:16-93:2].

288. Mr. Hedberg further explained that if administrative user access is not properly restricted, "[i]t increases the risk for unauthorized access to certain information." [SEC Ex. 55 [Hedberg Dep.] 93:3-10].

289. When asked how important it was that the software companies that he evaluated have authentication and authorization practices, as discussed in the Security Statement, [Ex. A to JS at 3], Mr. Thill acknowledged that it was "[v]ery important" to him. [SEC Ex. 56 [Thill Dep.] 61:20-62:7].

290. According to Mr. Thill, it is important that "who says they're getting in is actually who is getting in and that these passwords aren't shared, that they're individual to each…user." [SEC Ex. 56 [Thill Dep.] 62:8-17].

291. When asked how important it was that the software companies that he evaluated follow password best practices, as discussed in the Security Statement, [Ex. A to JS at 3], Mr. Thill acknowledged that it was "[v]ery important." As Thill explained, complex passwords are important because when passwords are simple, "bad guys can get in." [SEC Ex. 56 [Thill Dep.] 62:18-63:14].

292. When asked how important it was that the software companies that he evaluated follow vulnerability testing, as discussed in the Security Statement, [Ex. A to JS at 3], Mr. Thill acknowledged that it was "[v]ery important." [SEC Ex. 56 [Thill Dep.] 68:17-21].

293. When asked how important it was that the software companies that he evaluated follow penetration testing, as discussed in the Security Statement, [Ex. A to JS at 3], Mr. Thill

acknowledged that it was "[p]retty critical." As Thill explained, penetration testing is important because "[o]nce you build the software, you got to ensure that the bad guys can't get in." [SEC Ex. 56 [Thill Dep.] 70:2-22].

294. In his deposition, Mr. Thill acknowledged that it would be concerning if a software company did not have a Security Statement. As Mr. Thill explained, since "everything is being put on top of these platforms to run our economy[,]…software companies are expected to have…the basic locks and bolts to ensure that consumers and enterprises are protected." [SEC Ex. 56 [Thill Dep.] 49:8-21].

Dated: June 13, 2015

Respectfully submitted,

/s/ Christopher M. Bruckmann

Christopher M. Bruckmann
Christopher J. Carney
Kristen M. Warden (admitted *pro hac vice*)
John J. Todor (admitted *pro hac vice*)
William B. Ney (admitted *pro hac vice*)
Benjamin Brutlag
Lory Stone (admitted *pro hac vice*)
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549
202-551-5986 (Bruckmann)
202-551-2379 (Carney)
202-551-4661 (Warden)
202-551-5381 (Todor)
202-551-5317 (Ney)
202-551-2421 (Brutlag)
202-551-4931 (Stone)
BruckmannC@sec.gov
CarneyC@sec.gov
WardenK@sec.gov
TodorJ@sec.gov
NeyW@sec.gov
BrutlagB@sec.gov
StoneL@sec.gov

Attorneys for Plaintiff
Securities and Exchange Commission

CERTIFICATE OF SERVICE

I hereby certify that on June 13, 2025, I electronically filed the foregoing document with the Court via CM/ECF, which will automatically send notice and a copy of same to counsel of record via email.

/s/ Christopher M. Bruckmann
Christopher M. Bruckmann